REMARKS

In accordance with the foregoing, claims 11, 14, 15, 17, and 20 are amended. Claim 22 is added. No new matter is added. Claims 12, 13, 16, 18 and 19 are cancelled without prejudice. Claims 11, 14, 15, 17 and 20-22 are pending and under consideration.

CLAIM REJECTIONS UNDER 35 U.S.C. §112

Claims 16, 18 and 19 are rejected under 35 U.S.C. §112, second paragraph. Claims 16, 18 and 19 are cancelled herewith which renders the rejection moot.

CLAIM REJECTIONS UNDER 35 U.S.C. §102

Claims 11 and 12 (the Office Action erroneously indicated that claims 1 and 2 are rejected, but claims 1 and 2 have been cancelled) are rejected under 35 U.S.C. §102(a) as allegedly being anticipated by U.S. Patent Application Publication No. 2003/0009659 to DiSanto et al. (hereinafter "DiSanto").

Independent claim 1 is amended herewith to include the features originally recited in claims 12 and 13, which are now cancelled, and other features. The claim amendments are supported by the originally filed application. No new matter is added.

Amended independent claim 1 patentably distinguishes over DiSanto at least by reciting "a modem connection unit, used when said security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of the gateway and another second telecommunication terminal." Applicants respectfully direct the Examiner's attention to the fact that the claimed modem unit achieves a transfer of encryption technologies from the packet oriented network into public telephone network.

DiSanto discloses a security device for secure communication over a plurality of networks (see DiSanto's Abstract). The internal modem 240 in FIG.2B of DiSanto is used to perform analogue to digital conversion when digitized voice data is directed to port 245 (see paragraph [0033] of DiSanto). Thus, the modem 240 is used merely to comply with the technical requirements of a respective network, but not to provide a technical solution enabling encryption of voice data in a heterogeneous network including a packet oriented network and a telephone network.

Furthermore, amended claim 1 now specifies that "a point-to-point protocol connection is used over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol." The Office Action alleges that this feature originally recited in claim 12, is anticipated by "a procedure for establishing a direct connection between two nodes" disclosed in DiSanto. However, unlike in DiSanto, the modem of the claimed security module enables a "telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network, and at least one second telecommunication terminal in a telephone network." The procedure for establishing a direct connection between two nodes in DiSanto does not anticipate or render obvious this type of connection among terminals of different networks.

Additionally, claim 11, as amended specifies that "the encrypted transport protocol is Secure Real Time Transport Protocol." The Office Action takes the position that this feature, which was previously recited in claim 13, is rendered obvious by a general statement in the prior art that "applications for securely transmitting voice data through networks [...] should employ SRTP" (see the last paragraph on page 4 of the Office Action). However, the Office Action does not consider the claim as a whole, including the preamble, which specifies that the security module is used "for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network, and at least one second telecommunication terminal in a telephone network that is at least one of analog and digital and is connected to the packet-oriented network via a gateway." Thus, the encrypted transport protocol being Secure Real Time Transport Protocol in such a heterogeneous network and the features of security module are not rendered obvious merely by the above-reproduced statement which is a prior art recommendation in vacuum, with no relation to the environment in which the claimed secured module functions.

At least for the above reasons, amended claim 11 and pending claims 14, 15 and 17 depending from claim 11 patentably distinguish over the prior art.

CLAIM REJECTIONS UNDER 35 U.S.C. §103

Claims 13-21 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over DiSanto in view of the article "*Conversational IP multimedia Security*" by Blom et al. ("Blom").

Blom does not correct or compensate for the above-identified failure of DiSanto to anticipate or render obvious <u>all</u> the features recited in amended claim 11. Therefore, pending claims 14, 15 and 17 depending from claim 11 are patentable at least by inheriting patentable features from claim 11.

NEW CLAIMS

New independent claim 22 is directed to a security module used in a heterogeneous network including a IP-based Local Area Network and a public Time Division Multiplexing telephone network. The claim is supported by the originally filed specification. The security module patentably distinguishes over the prior art by reciting:

- a protocol processing unit enabling communication between terminals of the a IP-based Local Area Network using an encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, by converting voice signals received from a terminal of the telephone network into data packets for transport via the encrypted transport protocol, and converting data packets, arriving at said security module after transport via the encrypted transport protocol, into voice signals; and
- a modem connecting any telecommunication terminal of the telephone network with the protocol processing unit, to ensure communication between the telecommunication terminal of the telephone network and any terminal of the IP-based Local Area Network using the encrypted transport protocol.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: March 19, 2009

By: L Todor
Luminita A. Todor
Registration No. 57,639

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501